Algorithmes classiques

1 Division euclidienne par soustraction

Entrée : Deux entiers $a \geq 0, b > 0$.
Sortie : Le quotient dans Q
et le reste dans R.

$B := b;$
$R := a;$
$Q := 0;$
tant que $R \geq B$ *faire*
début
$R := R - B$;
$Q := Q + 1$;
fin ;

2 Division euclidienne version binaire

Entrée : Deux entiers $a \geq 0, b > 0$.
Sortie : Le quotient dans Q
et le reste dans R.

$N := 0;$
$Aux := b;$
tant que $Aux \leq a$ *faire*
début
$N := N + 1;$
$Aux := 2 * Aux;$
fin
$B := b;$
$R := a;$
$Q := 0;$

tant que $N > 0$ *faire*
début
$Aux := Aux/2;$
$N := N - 1;$
si $R < Aux$
alors $Q := 2 * Q$
sinon début
$Q := 2 * Q + 1;$
$R := R - Aux;$
fin ;
fin ;

3 Algorithme d'Euclide du PGCD

Entrée : Deux entiers a et b avec $b \neq 0$.
Sortie : Le PGCD de a et b dans R_0

$R0 := |a|;$
$R1 := |b|; \quad (b \neq 0)$
tant que $R1 > 0$ *faire*
  début
    $R := Reste\_Division(R0, R1)$;
    $R0 := R1$;
    $R1 := R$;
  fin ;

4 L'algorithme d'Euclide étendu

Entrée : Deux entiers a et b avec $b \neq 0$.
Sortie : Le PGCD de a et b dans R_0
les coefficients de Bézout dans U_0 et V_0
($aU_0 + bV_0 = PGCD(a, b)$)

$R0 := a;$ $\quad (a \geq 0)$
$R1 := b;$ $\quad (b > 0)$
$U0 := 1;\ U1 := 0;$
$V0 := 0;\ V1 := 1;$
tant que $R1 > 0$ *faire*
début
$Q := Quotient\_Division(R0, R1)$;
$R := Reste\_Division(R0, R1)$;
$U := U0 - Q * U1$;
$V := V0 - Q * V1$;
$R0 := R1$; $R1 := R$;
$U0 := U1$; $U1 := U$;
$V0 := V1$; $V1 := V$;
fin ;

5 Calcul d'une puissance

Entrée : Un nombre a et un exposant n
Sortie : a^n dans R
(On opère avec une loi associative $*$)

$A := a;$
$N := n;$
$R := 1;$
tant que $N > 0$ *faire*
  si N *pair*
    alors début
      $A := A * A;$
      $N := N/2;$
    fin
    sinon début
      $R := R * A;$
      $N := N - 1;$
    fin.

6 Les restes chinois

Entrée : Deux entiers m et n premiers entre eux
ainsi que deux entiers a et b.
Sortie : Une solution du système
$x \equiv a \quad (m)$
$x \equiv b \quad (n)$

$EuclideEtendu(m, n, U, V)$;
(ainsi $Um + Vn = 1$)
$X := Umb + Vna$